


# FLORIDA HIGHWAY PATROL

## POLICY MANUAL

	SUBJECT DIGITAL FINGERPRINTING – RAPID ID DEVICE	POLICY NUMBER 17.24
		ISSUE DATE 01/15/08
	APPLICABLE CALEA STANDARDS	REVISION DATE N/A
		TOTAL PAGES 6

### 17.24.01 PURPOSE

To provide guidelines for the issuance, training and use of the Rapid ID Digital Fingerprint Device.

### 17.24.02 POLICY

It is the policy of the Florida Highway Patrol to provide its members with the most current, cutting edge technology in the effort to apprehend criminals and fulfill its mission to provide the citizens of this state a safer Florida.

- A. The issuance and use of the Rapid ID Device (RIDD) is intended to provide members with a specialized tool to assist in the positive identification of individuals under appropriate circumstances.
- B. A Rapid ID Device (RIDD) may be used in a variety of circumstances; however, members must be aware that there are specific requirements and guidelines for its use.

### 17.24.03 DEFINITIONS

- A. **RAPID ID DEVICE – (RIDD)** A handheld, Wireless Supported Scanning device that communicates via the Mobile Data Computer (MDC) to the Florida Department of Law Enforcement Rapid ID (FALCON) system. The device checks two fingerprints obtained from suspects roadside against wants and warrants and can provide positive identification and a Criminal History if electronic prints exist in the Florida Department of Law Enforcement's Rapid ID (FALCON) system.

### 17.24.04 RESPONSIBILITIES

- A. Authority to issue or approve Rapid ID Devices to members shall be vested in the Director or his designee.
- B. Only devices which conform to the standards as set forth by the Florida Department of Law Enforcement will be approved.

- C. The Chief Training Officer at the Florida Highway Patrol Training Academy shall be responsible for overseeing the development and administration of the training process for assuring proficiency of instructors and operators with the Rapid ID (FALCON) Digital Fingerprint Device. This shall include but not be limited to:
  - 1. Ensuring lesson plans and any necessary forms are developed based on manufacturer's recommendations, Florida Department of Law Enforcement guidelines and appropriate legal mandates.
  - 2. Maintaining Training Records:
    - a. Ensuring that proficiency training is received by each user and;
    - b. Training is documented and forwarded to the Training Academy.
  - 3. Reviewing and revising all applicable training criteria on an as needed basis.
- D. Troop Training Coordinators shall ensure that each member provided a Rapid ID Device receives required training in the field and that:
  - 1. The original rosters and/or certificates are sent to the Chief Training Officer at the Florida Highway Patrol Training Academy and;
  - 2. A copy of the training rosters and/or certificates is placed in the member's troop personnel file.
- E. Troop Commanders shall ensure that supervisory personnel who manage members equipped with the Rapid ID Device:
  - 1. Make certain members follow established guidelines and procedures for the use and maintenance of the Rapid ID Device.
  - 2. Repairs and replacement of damaged or non-functional Rapid ID Devices are documented and performed as directed by the Chief Technology Officer.
  - 3.
    - a. All statistical reporting requirements are being completed as required to ensure adequate program evaluation.
    - b. On a monthly basis, reports involving cases in which the Rapid ID Device played in integral part in making an arrest shall be forwarded up through the chain of command to the Chief of the Bureau of Investigations.
- F. The Chief of the Bureau of Investigations or his designee shall be responsible for maintaining a system of tracking all cases which are sent from the field involving

the Rapid ID Device. Cases of interest, for example, are ones in which the Rapid ID Device enabled the member to make an arrest based on the fingerprint and not solely the running of an individuals name through FCIC/NCIC.

- G. The Chief Technology Officer shall be responsible for overseeing the technology portion of the Rapid ID Program.
  - 1. All Rapid ID Device units purchased by the Department will be approved, inspected and installed as determined by the Chief Technology Officer.
  - 2. Rapid ID Devices in need of repair or replacement shall be brought to the attention, via the chain of command, to the Chief Technology Officer.

#### **17.24.05 PROCEDURES**

- A. Issuance of the Rapid ID Device:
  - 1. A Rapid ID Device will be issued only to members that have had training on the operation of the unit. Training shall include considerations and requirements for use of the device under various circumstances.
  - 2. All Rapid ID Device units must be properly maintained in accordance with the manufacturer's recommendations as detailed in the training provided prior to use.
- B. Training
  - 1. Prior to issuance of a Rapid ID Device, members will complete a Department approved Rapid ID Device course and demonstrate proficiency on the unit.
  - 2. Training will be based on manufacturer's recommendations and suggestions from the Chief Training Officer.
  - 3. Training will include at a minimum:
    - a. Setup and maintenance procedures;
    - b. Proper use guidelines;
    - c. Legal issues involved with the use of the Rapid ID Device;
    - d. Reporting requirements;
    - e. Other issues as deemed necessary and established by the Chief Training Officer, Florida Highway Patrol Academy.
- C. Guidelines for Use of the Rapid ID Device
  - 1. The Rapid ID Device may be used in situations where the subject to be

fingerprinted has given a knowing and willing voluntary consent or permission for the member to use the device. This may include consent given during lawful encounters. (i.e.: traffic stop)

- a. As with other forms of consent, the consent can be limited or withdrawn at any point by the subject.
- b. If consent is withdrawn; use of the Rapid ID is **not** authorized and its use must stop immediately. Members shall not force or coerce anyone to submit to the scan.

- 2. The Rapid ID Device may be used in situations where reasonable suspicion can be articulated that the subject to be printed has committed, or is about to commit a criminal act, when there is a justifiable and reasonable belief that such printing via the Rapid ID will either establish or nullify the subject's connection with that crime. The key here is that the use of the Rapid ID Device is used as quickly as possible after reasonable suspicion is established.

- a. Failure to comply with the request to provide a Rapid ID scan under these circumstances may constitute a form of obstruction; however, it may be more appropriate to use the failure to comply as further evidence of suspicion for the suspect crime and simply proceed with the investigation without the scan.
- b. The Rapid ID may be used in situations where the subject to be printed would otherwise be required to give traditional fingerprint samples.

Some examples would include:

- 1. Probable cause criminal arrest situations.
  - 2. Required sentencing fingerprints for court.
  - 3. When a subject is issued a citation (if the citation requires fingerprint(s) to be affixed), a Rapid ID might be used to rapidly ensure the identity given by the subject matched his prints, since proof of his correct identity is already in question and is the cause for placing the print on the citation in the first place.
- 4. The Rapid ID may be used in situations where the use of the device has been specifically authorized pursuant to a valid subpoena; however, if the subpoena is not for immediate compliance, the subject should be allowed to appear for fingerprinting at the future time indicated on the subpoena.
    - a. Members should be aware that the subject may be able move

to quash the subpoena.

- b. Failure to honor a subpoena for Rapid ID use should be addressed in court and not be handled by attempting to force compliance via enforcement actions at the time of the refusal to comply.
- 5. The Rapid ID may be used in situations where the use of the device has been specifically authorized pursuant to a valid court order.
  - a. Where a court order requiring the use has been ordained, reasonable and safe efforts to gain compliance may be employed.
  - b. Failure to comply may constitute contempt of court and may constitute obstruction of justice.
- 6. Use of the Rapid ID Device for random or generalized investigative or intelligence gathering, with no focused case or other reason is **not** authorized. Special care should be taken to ensure devices are not used for purposes that may lend themselves to the inference of improper “profiling.”
  - a. Any specialized non-standard use of the Rapid ID Device shall require notification and authorization by the member’s immediate supervisor. If the immediate supervisor is not available, the request will be forwarded to the on-duty Shift Commander.
  - b. Examples of non-standard use may include:
    - 1. Request from an outside agency to fingerprint a suspect in custody. (As long as the requesting agency complies with the procedures set forth in this policy.)
    - 2. Traffic Homicide investigation in which there is no other identifying paperwork for the victim.
- 7. Guidelines cannot be written to encompass every possible application for the use of a Rapid ID Device. Members, therefore, should keep in mind the guidelines set forth in this policy to assist them in deciding whether the device may be used or not.
- 8. Members are expected to be able to justify, based on these guidelines, training, experience and assessment of the circumstances, how they determined that use of the Rapid ID Device was justified under the circumstances.